Information Operations

Future Force 2020 is the Army's benchmark for the integration of proactive and preemptive, full spectrum Information Operations (IO). *...those actions taken to affect the adversary, and influence others' decision making processes, information and information systems while protecting one's own information and information systems.*

Introduction: Information Warfare directed against the United States and its interests will improve in terms of sophistication and employment over the next quarter century. The greatest risk lies in the potential use of information warfare to attack and weaken our critical homeland infrastructure and military support systems and the use of information warfare by our adversaries to complicate and oppose U.S. military operations at every opportunity, undermine our international credibility and strive to weaken our sense of nationalism, purpose and resolve. As a result, the Department of Defense designated the U.S. Information Operations Command to consolidate Service networks; communications, information operations; intelligence, surveillance, and reconnaissance (ISR); and space functionalities. Networked activities on the battlefield contributed to the Joint network and therefore became Joint by design. Information Operations Integration into the modern battle space requires an increased flexibility in order to meet the multi-faceted missions the Future Force will encounter. In addition to maintaining an ability to fight a major action worldwide, Future Force IO is capable of managing multiple small scale contingencies, react to crisis action planning, provide support to stability operations, support operations humanitarian assistance, peacekeeping operations and home land defense missions. In the new Global Threat Environment, Army IO integrates with both military and civilian entities.

By 2020 changes in IO policy and legal restrictions; Army and Joint, Interagency, and Multinational IO definitions, are clearly defined as well as roles and responsibilities crossing the service boundaries, to include combined and multi-national components in order to be effectively and efficiently integrated into all military operations. These developments ensure that information and intelligence are shared in a timely and efficient manner and which allows the Future Force to perform critical roles in support of

the Joint Force Commander's (JFC) guidance on IO. Future Force IO uses innovative approaches to influence, shape, sustain and manage the modern battle space and is able to protect its critical C4, ISR and decision support infostructure. The Army provides significant portions of the Joint Force IO capability through the Army Information Operations Command or through the Army component of supporting specified commands. Future Force UA and UE unit's organic IO staff integrate full spectrum IO and draw from non-organic forces with IO capabilities to support planning and execution. It employs and integrates a sophisticated suite of technical and non-technical core and supporting IO capabilities.

IO Core Capabilities: The IO core capabilities include Electronic Warfare (EW), computer Network operations (CNO); consisting of Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE); Psychological Operations (PSYOP), Operations Security (OPSEC) and Military Deception. Supporting capabilities include physical attack, physical security, information assurance and counterintelligence, with the related capabilities of public affairs and civil military operations. The requirement for these capabilities inspired the development and implementation of innovative tactics, techniques, and procedures and in some instances materiel solutions. Information Operations leaders and soldiers employ these capabilities in a variety of ways to meet strategic, operational and tactical objectives. While core IO elements remain unchanged, new applications and improvements in technology make these elements more flexible and responsive to changing situations. Future Force 2020 will augment core IO capabilities by integrating IO-related actions, products and activities of supporting capabilities.

IO and Technology: The application of evolving C4, ISR, Space Control, decision support and related technologies provide IO quantitative advantages in collecting, processing storing, and transmitting information worldwide at unparalleled speed and fidelity. Cyber warfare operations demand exploitation of state of the art technologies to enable US computer network operations (CNO) to protect US information systems while taking advantage of vulnerabilities in the information systems of our adversaries.

Technological advancements (i.e. autonomous CNO, the ability to autonomously generate signals and signatures for deception; use of biometrics; avatars, voice recognition; language translation, etc.) provide the capabilities that make IO staff elements more flexible and responsive to changing situations and environments. These technological advancements significantly enable automated capabilities in Operations Security, Computer Network Defense, and Information Assurance to provide a far more capable IO defense, thus frustrating an adversary's attacks on our information systems while protecting our ability to exploit the Global Information Environment. Information Assurance is critical to maintain and protect the Component Commander's ability to transmit, store and use information and information systems. Cyber warfare operations demand exploitation of state of the art and emerging technologies to enable our computer network operations to protect our information systems while taking advantage of vulnerabilities in the information systems of our adversaries. Automated defense systems are less reliant on human interface to detect and defend against threat intrusion.

The Future Force of 2020 benefits in both the practice and technology required to execute effective OPSEC and Military Deception missions. New automated systems to generate signals and signatures for deception, and automated systems to detect electronic fugitive transmissions for OPSEC, are examples of technological advancements in equipment for success in these IO capabilities. Additionally, the effective integration of Civil Affairs (CA) and Public Affairs (PA) into the IO campaign is key to our success. Information Operations employments require the human interface that only these disciplines can offer. The development of a shared, automated database between IO and the supporting capabilities to use and exploit information regarding social, historical, ethnic, religious and cultural idiosyncrasies expedites the process of integrating the missions and functions of these fields.

The intelligence support to IO in the Army of 2020 benefit from an integrated, automated, database-sharing software capable of providing near real time, technical and non-technical intelligence to the synchronized IO effort including support to Civil Affairs and Public Affairs activities. When fully integrated and synchronized with

Information Management and Intelligence Surveillance and Reconnaissance, IO enhances joint battle command and allows the Future Force to implement decisions more effectively and more efficiently than ever before.

IO Force, Training and Education: While advances in technology will enhance our IO capabilities they can only be exploited with a trained and equipped IO force ready to seize the advantage. Although IO planning and integration staffs will be included in all Future Force 2020 units, the greater preponderance of IO and IO support capabilities will reside in specifically designed OF 2020 units focused foremost on providing a broad range of IO support at the Army Service Component Commander, Joint Task Force, Land Component Commander level The IO force of 2020 is a flexible organization trained to serve in a wide array of technical and non-technical strategic, operational, and tactical branch assignments. Future Force 2020 recruits, develops, trains, and retains a professional full spectrum IO force prepared to meet any challenge. The IO force is skilled areas of Electronic Targeting, Electronic Fires, Electronic Security, Computer Network Operations, Operations Security, Psychological Operations, Military Deception, Media Assessment, Human Factors Assessment, Counter-IO, Counter-ISR, Measure of Effectiveness Assessment, Vulnerability Assessment, and Critical Infrastructure Protection in addition to maintaining a broad familiarity with such subject areas as Civil Affairs, Public Affairs, Information Assurance, Intelligence Support, and Physical Destruction.

The Future Force IO staff is a skilled mix of Active Component/Reserve Component (AC/RC) soldiers, civilians and contractors serving in a wide array of technical and non-technical strategic, operational, and tactical branch assignments. A standardized approach to training and education through classrooms, on-the-job-training and distance learning are used to ensure that only qualified personnel are assigned to IO positions within the Army. Information Operations leaders and soldiers conduct comprehensive IO training in the unit to exercise and perfect their IO knowledge and skills during Army, joint force exercises, pre-deployment training and enroute rehearsals. Army and Joint warfighting exercises stress IO staffs and operators

by providing units a diverse, complex and sophisticated information environment in which technical and non-technical IO problems are presented in and effort to complicate standard military operations and test unit readiness and competence to operate in such environments.

Summary: The Future Force of 2020 will employ IO as a core capability used to influence, shape, sustain and manage the battlespace and enable decision dominance thereby making it a key enabler for joint battle command. The operational environment demands a force prepared to exploit the synergistic advantages stemming from the integration of the full spectrum of IO. The embedded IO staff of the Future Force integrates full spectrum IO planning, directing and execution functions. These integrating staffs draw their direct and general support from a dedicated IO force structure comprised of units capable of providing a broad range of support to the ASCC, JTF and LCC. Commanders and staffs integrate all information and information-based capabilities across the full spectrum of operations. Advanced technology, major capability improvements and shared database development programs and intelligence fusion ensure decision superiority by which the joint force, not only has complete real-time visibility of the relevant portions of the information environment, but also a robust analytical capability to identify patterns of attack and defense. OPSEC, CND, and IA state of the art and beyond automated capabilities technology improvements provide a much more capable IO defense, thus frustrating an adversary's information, information systems and decision making while protecting our own. Advanced skills in cyber-warfare, the ability to deal with sociological and demographic realities, and the integration of all forms of attack on adversaries' decision systems provide the Future Force with full spectrum information operations effects.